Evaluation Criterias for Trust Management in Vehicular Ad-hoc Networks (VANET)

Qasim Alriyami and Asma Adnane and Anthony Kim Smith
School of computing and mathematics
University of Derby
Derby, UK
Email : q.alriyami1, a.adnane , a.k.smith @derby.ac.uk

***Abstract*—Vehicular Ad-hoc networks (VANETs) have been around for a short time with a very promising future ahead. VANETs are one of the ad hoc networks real-life applications, where vehicles communicate which each other and with fixed components known as roadside units. VANETs have their unique characteristics and requirements which differ from those in standard ad-hoc networks, but the security remains a major challenge because of the very dynamic topology and the lack of infrastructure. In this autonomous and auto-organized environment, the question of whom to trust and for what become very important and difficult to answer. This paper addresses the issues associated with establishing trust between peers in VANET. It defines, discusses and evaluates various trust management approaches and how they address VANET requirements. The paper also proposes criterias for assessing the effectiveness of trust management models with regards to challenges specific to VANETs.**

I. Introduction

VANETs are a subset of ad-hoc networks and share many advantages and challenges with other types of similar networks such as mobile ad-hoc networks (MANETs) and Wireless sensor networks (WSN). VANETs have two main components: vehicles with wireless communication capabilities, and Road Side Units (RSUs). The road side units form the VANET infrastructure, they can be generally found in service stations, traffic lights and selected points along the road side [8]. VANETs are designed to facilitate Vehicle-to-Vehicle (V2V) and vehicle to infrastructure (V2I) communications.

There are many applications for VANET such as increasing road safety, and driver luxury. Parno & Perrig have presented a safety application called "*Crash Avoidance*" [1]. This application is based on sharing information about the current road conditions and congestions. In fact, it is estimated in one year that 630,000 crashes in the United States are caused by sudden lane changes or merges, which can be prevented if cars can communicate their location information with other vehicles [1]. Other applications for VANETs are dedicated to the comfort of the driver such as the ability to access the internet, multimedia and social networking websites [2]. All these applications suffer classic network security challenges as well as challenges inherited from ad-hoc networks.

Many research projects have been conducted on VANET security among other concerns such as routing and Quality of Service (QoS). VANETs are vulnerable to many insiders and outsider attacks because of their open nature. Trust has been considered as the key element in these networks, where nodes do not rely on any centralised administration, and they have to cooperate and work together in order to maintain the network services. Each node need a certain level of knowledge about the willingness and the availability of the other nodes in performing correctly a certain action in certain circumstances. This knowledge is called trust. Yet, in the literature, there is no consensus on the definition of trust. As a result, a multitude of formal models for trust calculation and management have emerged. However, this also leads to a certain conceptual confusion indicated by the fact that similar concepts appear under different names and reciprocally.

The concept of ad-hoc networks has emerged very quickly, and many trust models have been designed to ensure two important requirements for the good functioning of these networks which are cooperation and security. Indeed, the cooperation enforcement protocols ensure that all the system entities are cooperating [3], and the security protocols ensure that only authorised entities are in the system, and their communications are secured [4].

However, the lack of fixed infrastructure and the dynamic topology make the cooperation between nodes in ad-hoc networks harder to establish than in conventional networks. Indeed, security solutions for these networks must be based on distributed, auto-organised and cooperation enforcement mechanisms [5]. The cooperation between nodes of ad hoc network is a major challenge, because routing and securing control messages in any ad hoc network require the cooperation between all the network nodes. In fact, many security attacks originate due to the selfishness of some nodes that try to use the resources of the network for their own benefits [6]. Trust management is than very crucial because nodes acting on false information from untrusted peers may lead to catastrophic results [7].

In addition, VANETs have special requirements such as the rapid mobility and delay intolerant which require different security approaches than those adopted in the other ad-hoc networks. For example, Users' privacy must be ensured, in order to encourage users to join VANET networks while protecting their identities from being traced at the same time. However, establishing trust between vehicles while keeping the identity of the driver anonymous is another major challenge in VANETs. This paper investigates the issues of trust management, and proposes some criteria for evaluating trust models for VANET. The paper is organised as follow: section 2 presents trust theories. Section 3 highlights the challenges associated with securing VANETs. While, section 4 examines

previous work proposed in the area. Section 5 concludes the paper by introducing the benchmark or evaluation criteria for trust management.

II. Trust theories

The study of the formalization of trust as an automated concept was first introduced two decades ago by Stephen Paul Marsh [11]. Marsh is considered a pioneer in the subject of trust in intelligent systems, he argued that artificial agents should have the capability to make sensible and informed decisions on who is and who isn't trustworthy. His novel idea was to allow intelligent systems to make informed decisions relying entirely on information presented in a particular situation. This means that trust is an impeded feature in smart agents to allow informed decisions based on available information. Further to his studies on the formalisation of trust, Marsh conducted further research with Briggs on the different flavours of trust [12] . They argued that trust is not a simple dual sided concept but it is rather a complex one. In theory the smart agent can simply decide to trust or not trust another agent. But in reality, the most likely decision would be to trust the other agent to some degree and decide where to go from there in a concept referred to as "initializing trust".

Most of security trust-based solutions focus on reputation and recommendation models, which are commonly used for example in e-commerce applications and cloud computing [13], [14]. The implementation of these models is based on a central trusted entity (e.g. Certificate Authority). This entity will have the authority to supervise the behaviour/transactions of any participant (in the system or network), and evaluate him with a reputation value. A participant reputation will help the other participants to decide whether or not to cooperate with him and trust the data he provides. As only the trusted authority is able to provide this reputation, all the anticipants will trust it and take it as a valid information without any verification. In ad hoc networks, these authorities are not an option because they do not exist at all times. Trust solutions for MANETs are the basis for all similar research in VANETs, even though models cannot be directly applied to the later. One of the challenges is that trust models in MANET make the assumption that trust is available before a route is established between two nodes [7].

Other challenges for trust management in VANETs as highlighted by [7] and [8] include verifying trust data in real-time. Nodes are required to act on information about accidents and road conditions immediately any delay may render the information useless. Nodes in congested metropolitan areas have to process a large number of messages which could be an overwhelming task. VANETs are exposed to sophisticated false identity attacks such as Black-hole and Sybil attacks which makes establishing trust harder in the presence of malicious nodes. Finally, revealing the real identity of drivers can compromise their privacy which means establishing trust should not be based on information about the driver. Any trust management proposal should take all these issues in consideration and find a solution suited for VANETs. In this paper, we will be studying all these issues and their impact on establishing trust in VANET.

III. Characteristics of VANET

As mentioned earlier, the main focus of today's VANET applications is largely towards satisfying the drivers' desires for a safe and comfortable journey. These applications rely on the availability of road side units and the cooperation of other vehicles on the road. Information exchanged between vehicles should be secured from malicious nodes that try to attack these networks because of their open wireless nature. This makes integrity the most important security aspect in VANETs [13]. Information received from malicious untrusted nodes could harm the network operations. To understand how to secure these networks, we need first to see what makes them distinctive and vulnerable. VANETs have their unique properties when compared to other ad-hoc networks [6] [8]. These are the source of several security concerns in VANETs but are not of major burden in other ad-hoc networks.

A. Decentralized open systems

The purpose of VANET is to establish connection between nodes without the permanent need for fixed infrastructure. However, the lack of central management entity causes many challenge for these networks in message routing, QoS and security [30]. That is why solutions in ad-hoc networks are based on cooperative and distributed architecture and the same can be said for VANETs. Establishing trust between nodes cannot rely on a central authority for authentication, key exchange or certification [7]. So it is clear that decentralization is one of the most important characteristics, yet it poses a challenge for researchers to apply security and trust models.

B. The authenticity of information

It is very important to insure that messages are authentic because some of this information is used in making life and death decisions. The integrity of messages broadcasted in VANET must be checked by linking them to an authenticated (trusted) source to avoid identity attacks like the Sybil attack [1]. However some user information is private and should be kept that way, which introduces a challenge for trusting authenticated users while keeping their identity anonymous. Linking a user to an identity is very important for forensic evidence as highlighted by [1]. But it is vital that this information should be Limited to government and law enforcement agencies. Some solutions don't require knowledge of the identity to authenticate certain messages and can verify the integrity of the message based on its contents [4].

C. Real-time processing

The success of VANET relies on the availability of information in Real-time, so any interruption or delay in the delivery might affect the validity and the usage of the message. VANET should follow strict security requirements to ensure the privacy, confidentiality, non-repudiation while guaranteeing the integrity of the message delivered in real-time [2]. These networks are delay intolerant which makes the availability and trust worthiness of other nodes to carry the message across crucial for safety applications [20].

D. Highly Dynamic Topology

VANET consists of fast mobile vehicles in pre-determined paths (roads). According to [5], when vehicles travel in highways with an average speed of 60 mph they only come in contact with other nodes for a very short time (5 Seconds). This makes the network topology very dynamic with nodes entering and leaving the network rapidly. This is a challenge for trust management since nodes have to make fast decisions with as little information as possible. The rapid mobility will also cause frequent network outage for vehicles traveling in remote areas [8]. The frequent changes in topology require solutions that do not involve prior knowledge of the other node and only examine the message carried across.

E. Routing

Message routing in ad-hoc networks rely on cooperation between nodes in the absence of central routing infrastructure. Fen and Wang [5] argues that high-speed and patterned mobility should be taken in consideration when designing a routing protocol for VANETs. Because unlike MANETs, a node cannot be expected to keep a routing table due to the highly dynamic nature of the network. The most well researched routing protocols inherited from MANET are proactive and reactive protocols [15]. Routing protocols in VANET can be further broken down in six categories: Position-based, Topology-based, Geocast-based, Broadcast-based, Cluster-based and Infrastructure-based [5] [10]. Most researchers recommend the use of position based and geocasting [15] for security and performance reasons but it all depends on the specific case in VANET.

F. Privacy

It is important to ensure that messages in VANET are not intercepted or modified by malicious hackers. Information such as the name, address of the driver and their locations' history is considered private. A successful solution should be able to address security while preserving the privacy of the drivers and their passengers [6]. The biggest challenge for drivers is to make decisions based on information they receive from vehicles they have no prior knowledge or experience with.

IV. Trust management in VANET

VANETs core operations are based on cooperation between nodes to relay messages through their neighbours. Generally, nodes are cooperative, but certain nodes will require some kind of incentive to cooperate, this might be because they have limited resources, or they are selfish. If nodes can't guarantee the delivery of their messages by a certain neighbour, they might refuse to trust him and to cooperate with him in the future. Existing trust models in VANETs can be broken down into three categories based on the source of information [7] [8]: - Direct trust: This type of trust is based on direct knowledge of the other node from previous encounters.
- Indirect trust: This is based on information received from other directly trusted nodes. So trust can be seen as a transitive attribute.
- Hybrid: This combines information locally stored with trust information exchanged with other nodes.

A. Trust-based Routing Protocols

Since routing is the most important aspect of operations in VANET, some trust solutions are built on top of routing protocols. One of the secure routing approaches is the CONFIDANT protocol [16], where the authors introduce the watchdog and pathrater mechanisms for routing in mobile ad hoc networks. The watchdog is a monitoring service, which calculate the reputation of each node based on its cooperation in the routing. The pathrater is a route selection mechanism, which uses the reputation as a metric in the route selection, so only trusted and cooperating nodes will be used for routing. Since CONFIDANT was designed for classic ad-hoc networks it has some limitations when applied to VANETs. One being that it does not scale to very large and dynamic networks like VANETs, and It does not address the frequent packet drops caused by changes in topology as experienced in VANETs.

SAODV is another secured routing protocol for ad hoc networks [19], it is based on AODV (AD-Hoc On demand Distance Vector). This protocol uses a public key infrastructure, and uses the digital signature to ensure messages' integrity. Just like AODV, SOADV suffers from large packet overhead which increases significantly with mobility. The overhead is also increased when using asymmetric cryptography which can lead to DoS in low resources nodes [17]. But, since power and storage are not a major concern in VANETs, SAODV is a promising trust solution. The Road Side Units (RSU) can be used as a central trusted system for key management. Nevertheless this will be always limited to areas where RSU is present. Another drawback of public key infrastructure is that the identity of nodes can no longer be kept private.

Adnane et al. [4] present a trust-based version of the OLSR protocol (Optimised Link State Routing Protocol). They show how trust-based reasoning can allow each node to evaluate the behavior of the other nodes, and to check the consistency of the routing information. In fact, each node uses a number of rules to verify the validity of the network topology by correlating all the received information from the network. This protocol doesn't generate an extra overhead to the network compared to the basic OLSR protocol, but applying the trust rules and verifying the consistency of all messages will require more time from each node, which might be a problem in VANET. When compared to AODV, OLSR generates more overhead, However OLSR protocol has a lowest delay in high mobility scenarios, this may be explained by the fact that OLSR is a proactive protocol [21], [22].

B. Trust models for VANETs

The authors in [7] and [20] have categorised trust models in the literature in three main categories: Entity-oriented, Data-oriented and combined or hybrid trust models. We agree with their categorization as it clearly groups the models in a logical manner according to how trust calculations are performed. Entity oriented trust is also referred to as direct trust which is based on information about the identity (node). While Data-oriented trust models focuses more on evaluating the content of the message to make the trust decision. Finally, the combined trust models are based on direct observations and on the other peers recommendations.

a) Entity-oriented Trust models: : in this category, models define trust as a combination of multiple factors about the entity. For example, Gerlach proposed a social trust model which uses calculations based on the principles of trust and confidence tagging, the overall trust value of certain node is calculated from the data available about the current specific situation (called *situational trust*), combined with the node's own belief (called *dispositional trust*) and the system in which the two nodes reside (called *system trust*). One of the drawbacks is that the author did not provide information on how the different types of trust are combined in the architecture.

Minahs et.al proposed another expanded trust model based on the node's roles and reputation [24]. In fact, their model combines role-based trust, experience-based trust, majority-based trust and priority-based trust. Role-based trust is derived from predefined roles while experience-based trust is calculated from direct interactions. Majority trust is formed based on opinions gathered from selected advisors. Priority-based trust is the value given based on the source of the trust information. One drawback with this model is that it relies on public key cryptography to determine role based trust (i.e. the role of the node is taken from the provided certificate). It requires a certificate authority to manage and validate keys. While, the above two models have some common aspects, the model in [24] is more valid for VANET as it has the ability to incorporate the time and location of the source node and has a majority agreed value for each node.

b) Data-oriented Trust models: : This type deals more with the trustworthiness of the data received from other nodes rather than the nodes themselves . Two examples of such models can be found in Raya et.al [25] and Golle et .al [26]. Both models are based on the fact that associations between nodes in VANETs are "short-lived" and take place in "volatile" environments. Raya et.al argued that the identity of the node in VANETs is irrelevant compared to the received information such as traffic conditions updates and safety warnings citeRaya2008. The model uses Bayesian inference (data fusion technique) and Dempster-Shafer Theory (evidence evaluation inspired by human reasoning) to evaluate the probability of an event taking place in a particular time and context. The model uses various evidences to calculate the probability of an event being correct in a particular time, location and context. The drawback in this proposal is that trust is purely based on events and it needs to be established every time an event or message is received from an entity regardless of any prior interaction with that entity. Another drawback is that it requires the evaluation of certain information (evidences) which could be tampered with or unavailable when needed.

In [26], Golle et.al took the approach of giving a score to each piece of data based on explanations gathered by a local agent. The local information agent resides at every node and contains the node's knowledge of the VANET. When information is received the agent evaluates it against what is already known. The agents have sensors that apply the basic rules of physics and statistical properties of events. For example (two nodes can never occupy one location at the same time) and (nodes rarely travel faster than 100 mph. This model also provides attack detection techniques especially for sophisticated attacks such as the "Sybil attack". This gives the model an advantage on VANET over the model proposed by Raya et .al [25]. The drawback in this model is the assumption that each node has a global knowledge of the network which in practise is not feasible. But if we assume that road side units can be trusted to have this type of knowledge then, this solution would be very applicable.

c) Combined Trust Models: : this type of trust models combine the trustworthiness of the nodes and the reliability of data presented. Dotzer et.al [27] proposed a reputation model inspired by the idea of "Opinion Piggybacking" (each node adds its own opinion about the message). Their proposed algorithm allows nodes to generate their own opinion on the message based on the collected data from previous hops. A node can have direct trust on other nodes from previous encounters or use other's opinions to formulate new trust values. When a new node first enters the network it can evaluate trust based on the actual message and not the source which makes feedback from others useful. Trust is dynamic and uses the geo-location of the reporting node and the timestamp on the message. The model also incorporates information about the surrounding environment in the network and the context in which the message was created. The shortcoming in this approach is that it is vulnerable to collision between nodes to affect the reputation system. In the model presented by Patwardhan et.al [28] trust is calculated based on node reputation and message data validation. The trustworthiness of previously unknown node is based on a value provided by trusted "anchor nodes" which have well established identities in the network. This model has the ability to validate message content by examining multiple factors such as: the location, the source of the message and the proxy providing it. A message validation algorithm is used to detect any malicious nodes. One of the drawbacks of reputation based models is that they rely on the existence of other peers that have enough knowledge and can be trusted. VANETs could make use of RSUs to be the trusted anchor nodes. But, If they do not exist than it becomes harder to calculate the trust based only the content of the message. Another model was proposed by Sahoo et.al [29] for secure VANETs routing inspired from Ant Colony. The model proposed an algorithm for clustering nodes in a VANET and choosing a cluster head that facilitates the routing process. When a source node (S) would like to send a message to a destination (D) within the cluster it first start by contacting the cluster head (CH). The cluster head calculates indirect-trust taken value from nodes within range and adds that to the direct-trust or knowledge of the source. The disadvantages of this proposal is that it assumes that nodes should be traveling in the same direction to form a cluster and the process for choosing a cluster head is time consuming.

To conclude this section, all these solutions designed particularly for VANET don't cover all the security requirements. This gives good opportunity for further research in the area, and a good starting point would be to understand all the advantages and flaws of the current solutions and evaluates them with a benchmark.

V. Evaluation criterias for the trust models

The above trust models have different approaches to address common ad-hoc characteristics in VANETs. The main requirements in VANETs are the integrity of information and cooperation between nodes to route messages. This paper

proposes the following list as criteria for evaluating affective trust management solutions in VANETs which is combined from [7], [8], [17] and [20]:

A. Decentralization

Trust management solutions should be distributed among nodes without the need for a central entity. The lack of infrastructure means that centralized solutions have less chance of being successful. Conventional cryptographic solutions require a central entity for key management such as a certificate authority (CA). To solve this we need a distributed key management solutions such as "Threshold Cryptography" which was proposed by Adil Shamir of (RSA) [8]. The concept of threshold cryptography is to share the secret key between n' entities with t' entities required to put together the secret key. This will solve the need for a central trust management entity but might not be practical for VANETs as there will not always be t parties present. The solutions proposed in [24], [25] and [28] do not require a central entity for trust management while [23] and [29] makes use of RSUs as a central administration entity. Since both approaches have their pros and cons, the best solutions is to have a dynamic key management solution that can toggle between both threshold cryptography and central PKI.

B. Adaptive to rapid network Changes (topology)

Vehicles travel relatively in high speeds making VANET topology very dynamic as links are dropped and new links are established. Nodes should not be expected to save trust association with other nodes for a very long time. Models in [25], [27] and [28] consider the short lived association between nodes and make their decisions on information rather than the entities delivering them. While other solutions came short when addressing this issue. The best solution would be to adapt rapidly to network changes and do not require prior knowledge of the network and its nodes.

C. Minimal Information to make a decision

In many cases there are very few vehicles in a VANET and a node may have no prior knowledge on any of the other nodes. Trust establishment mechanisms should be very quick and require little knowledge of the network to make a decision. Pure entity based models such as [23] and [24] are not very useful in these circumstances. The best solution to this would be like the models proposed in [26] and [29] where the trust decision is entirely based on the situation or context. While reputation based models such as [27] and [28] also have the disadvantage of requiring information from others who might not be always present. A good solution should consider very minimal input to make a trust decision and adjust the score as more information exist.

D. Scalability

In many ad-hoc networks there is no pre-set limitation on the number of nodes that can join the network as always is the case in VANETs. The trust solution should not be limited to a small number of nodes and should have the ability to expand to larger networks. Big networks pose the challenge of the enormous amount of information received from many sources in which the node is required to make a quick decision. Only few of the above models address scalability in their design. In the model proposed by Minhas et.al [24], a node has the ability to fix the number of peers to exchange trust related information. Dynamic Transmission Range is proposed in [29], where vehicles can adjust their wireless connectivity range to reduce the work load and preserve bandwidth (e.g. in case of traffic congestion). An ideal solution should be able to adapt to small and large networks.

E. Privacy

The biggest dilemmas in VANETs are how to trust information from unknown sources while keeping driver identity anonymous. Information stored and processed in vehicles include the name of the driver/s, their travel history and their permanent home address. This information should not be shared with others. Among the above solutions, [24] and [27] mentioned privacy briefly but did not specify exact measures. The models in [23] and [26] proposed algorithms that filter user sensitive information and prevents their exposure to others. The identity of the node in data-based solutions is irrelevant giving them a slight advantage over other solutions in this area.

F. Robustness/Security (against known attacks)

Ad-hoc networks are exposed to a wide range of malicious attacks that could obstruct the entire operations of the network. Robustness refers to the system's ability to stand different type of attacks. Models that rely on node reputation from others are more vulnerable to collision attacks where more than two nodes "bad mouth" other nodes [7]. Other models maybe vulnerable to more sophisticated attacks such as the Sybil attack and Illusion attacks [2]. Unfortunately most of the models examined did not address robustness except [26] and [29]. A good trust model should be tested against most frequent attacks (e.g. Sybil and Black hole).

G. Real-time processing

Trust models should have the ability to process information in real-time because VANETs require making very fast decisions. Trust management fail when the time required for making a decision is larger than the total encounter time with the other node which is usually very short. Some of the above models use time-stamps to validate the integrity of the message especially when the source is previously unknown [24], [25] and [27]. We need to remember that VANETs are delay intolerant networks and trust solutions should take this in consideration.

H. Realistic

Most researchers in ad-hoc networks proof their theories and models through simulation. Vehicular network Simulators can present packet level simulation of a VANET. But they require many mobility models and are always limited in the number of nodes and simulation runs [30]. This makes simulations limited compared to real vehicular test beds. The models presented in this paper all obtained their findings from simulation runs with limited mobility models. Furthermore, some of the assumptions made by the researchers results in the models not feasible for real road scenarios such as

the assumption that anchor nodes are always present in [28] and the assumption that a node has global knowledge of the network in [25].

I. Low Network Overhead

Bandwidth in wireless networks is limited by default. Solutions to secure ad-hoc networks must have a low packet overhead. Some of the models described above use public key infrastructure which introduces large overhead to the network [19], [24] and [28]. Network overhead can also be caused by continuous routing and security updates as in [16], [27] and [29]. Solutions should aim for the lowest overhead possible by reducing the amount of data exchanged with neighbours.

VI. Conclusion

This paper highlights the characteristics of VANETs inherited from conventional ad-hoc networks and others that are specific to vehicular networks. Successful operations of these networks rely heavily on collaboration between nodes which require trust and incentive. We covered the issue of trust management as one of the challenging security concerns as presented in the literature. We introduced the concept of trust in multiagent systems and how it has evolved in ad-hoc networks as a solution to many of the security concerns. Multiple trust solutions designed for VANETs were surveyed and critically described in details. The contribution of the paper is in the evaluation criteria for trust management solutions in VANETs. These criteria aim to set some baselines for researchers who wish to address the challenges of trust between vehicular nodes. They represent the collective efforts of several research papers in a single resource with an in-depth analysis of each category. A possible future work would be to look at potential improvements in some of the current trust models based on the evaluation criteria presented.

References

[1] B. Parno and A. Perrig, *Challenges in securing vehicular networks*, In Workshop on hot topics in networks (HotNets-IV), pp. 1-6, 2005.

[2] M. Al-kahtani, *Survey on security attacks in Vehicular Ad hoc Networks (VANETs),* IEEE 6th International Conference on Signal Processing and Communication Systems, pp. 1-9, 2012.

[3] P. Michiardi and R. Molva. *Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks*. Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security, pp.107-121, 2002.

[4] A. Adnane, C. Bidan, and R.T. De Sousa, *Trust-based security for the OLSR routing protocol*. Computer Communications, Vol 36, pp.1159-1171, 2013.

[5] F. Li and Y. Wang, *Routing in Vehicular Ad Hoc Networks: A Survey,* IEEE Vehicular Technology Magazine, Vol 2, Issue 2, pp. 12-22, 2007.

[6] M. Raya and H. Jean-Pierre, *Securing vehicular ad hoc networks*, Journal of Computer Security, pp. 39-68, 2007.

[7] J. Zhang, *A survey on trust management for VANETs*, IEEE International Conference on Advanced Information Networking and Applications (AINA), pp. 105-112, 2011.

[8] P. Wex, J. Breuer, A. Held, T., Leinmuller, & Delgrossi, L. *Trust issues for vehicular ad hoc networks*. In Vehicular Technology Conference, 2008. VTC 2008, pp. 2800-2804, 2008.

[9] P. Lerchbaumer, A. Ochoa, and E. Uhlemann,. *Test environment design for wireless vehicle communications*, In Vehicular Technology Conference, VTC-2007. pp. 2214-2218, 2007.

[10] M. Benamar, N. Benamar, K.D Singh, and D. Elouadghiri, *Recent study of routing protocols in VANET: survey and taxonomy*, In WVNT 1st International Workshop on Vehicular Networks and Telematics, 2013.

[11] S.P. Marsh, *Formalising Trust as a Computational Concept*, Doctorate of Philosophy, University of Stirling, Department of Computing Science and Mathematics, 1994.

[12] S. P. Marsh and P. Briggs, Examining trust, forgiveness and regret as computational concepts. In Computing with social trust, pp. 9-43, Springer London, 2009.

[13] F. G. Màrmol, F. Gómez, and M. Q. Kuhnen, *Reputation-based Web service orchestration in cloud computing: A survey*, Concurrency and Computation: Practice and Experience, 2013.

[14] A. Jøsang, R. Ismail, and C. Boyd, *A survey of trust and reputation systems for online service provision*. Decision support systems, pp. 618-644, 2007.

[15] P. Ranjan, and K. K. Ahirwar, *Comparative study of vanet and manet routing protocols*, In Proc. of the International Conference on Advanced Computing and Communication Technologies, pp. 517-523, 2011.

[16] S. Buchegger and J. Y. Le Boudec, *Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks.*, 10th Euromicro IEEE Workshop on Parallel, Distributed and Network-based Processing. pp. 413-410, 2002.

[17] E. Fonseca and A. Festag. *A survey of existing approaches for secure ad hoc routing and their applicability to VANETs.* NEC network laboratories (28), pp.1-28, 2006.

[18] N. Nidhi and D. K. Lobiyal, *Performance Evaluation or Realistci VANET using Traffic Light Scenario*, International Journal of Wireless & Mobile Networks, 4(1), 2012.

[19] M. G. Zapata, (2002). Secure ad hoc on-demand distance vector routing. ACM SIGMOBILE Mobile Computing and Communications Review, 6(3), pp.106-107, 2002.

[20] S. Tangade, and S. Manvi, *A survey on attacks, security and trust management solutions in VANETs,* Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), pp. 4-6, 2013.

[21] G.Z. Santoso, K. Moonsoo,*Performance analysis of AODV, DSDV and OLSR in a VANETs safety application scenario*,14th International Conference on Advanced Communication Technology, pp. 57-60, 2012.

[22] E. Spaho, M. Ikeda, L. Barolli, F. Xhafa, M. Younas, M. Takizawa,*Performance Evaluation of OLSR and AODV Protocols in a VANET Crossroad Scenario*, IEEE 27th International Conference on Advanced Information Networking and Applications, pp. 577-582, 2013.

[23] M. Gerlach, *Trust for vehicular applications*, in Proceedings of the International Symposium on Autonomous Decentralized Systems, pp. 295-30, 2007.

[24] U. F. Minhas, J. Zhang, T. Tran and R. Cohen, *Towards expanded trust management for agents in vehicular ad-hoc networks*, International Journal of Computational Intelligence Theory and Practice, 5(1), pp. 3-15, 2010.

[25] M. Raya, P. Papadimitratos, V. D. Gligor, and J. P. Hubaux, *On data-centric trust establishment in ephemeral ad hoc networks*, IEEE the 27th Conference on Computer Communications INFOCOM 2008.. IEEE, pp. 39-68, April, 2008.

[26] P. Golle, D. Greene and J. Staddon, *Detecting and correcting malicious data in VANETs*, Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, pp. 29-37, 2004.

[27] F. Dotzer, L. Fischer, and P. Magiera, *VARS: a vehicle ad-hoc network reputation system*, Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, pp. 454-456, June 2005.

[28] A. Patwardhan, A. Joshi, T. Finin and Y. Yesha, *A Data Intensive Reputation Management Scheme for Vehicular Ad Hoc Networks*, 3rd Annual International Conference on Mobile and Ubiquitous Systems - Workshops, pp.1-8, July 2006.

[29] R. R. Sahoo, R. Panda, D. K. Behera, and M. K. Naskar, *A trust based clustering with Ant Colony Routing in VANET*, Third International Conference on Computing Communication & Networking Technologies, pp. 1-8, July 2012.

[30] P. Lerchbaumer, A. Ochoa, and E. Uhlemann,. *Test environment design for wireless vehicle communications*, In Vehicular Technology Conference, pp. 2214-2218, September 2007.